U.S. DEPARTMENT OF COMMERCE PATENT & TRADEMARK OFFICE

FB/O Form PTO-1390	Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under *35 USC 371*	Attorney's Docket Number MODL3001/JEK
		U.S. Application Number (if known) 09/926634
International Application Number PCT/EP00/04780	International Filing Date 25 May 2000	Priority Date Claimed 28 May 1999
Title of Invention DEVICES AND METHODS FOR BIOMETRIC AUTHENTICATION		
Applicant(s) for DO/EO/US Albert MÖDL et al.	Assignee	

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items under *35 USC 371*:

1. ☒ This is a **FIRST** submission of items concerning a filing under *35 USC 371*.

2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under *35 USC 371*.

3. ☒ This express request to begin national examination procedures *(35 USC 371 (f))* at any time rather than delay examination until the expiration of the applicable time limit set in *35 USC 371 (b)* and PCT Articles 22 and 39(1).

4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of the International Application as filed *35 USC 371 (c) (2)*.
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).

6. ☒ A translation of the International Application into English *(35 USC 371 (c) (2))*.

7. ☒ Amendments to the claims of the International Application under PCT Article 19 *(35 USC 371 (c) (3))*
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 *(35 USC 371 (c) (3))*.

9. ☒ An oath or declaration of the inventor(s) *(35 USC 371 (c) (4))*. (☐ Executed   ☒ Unexecuted)

10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 *(35 USC 371 (c) (5))*.

Items 11 to 16 below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under *37 CFR 1.97* and *1.98*.

12. ☐ An assignment document for recording. A separate cover sheet in compliance with *37 CFR 3.28* and *3.31* is included.

13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. ☒ Other items or information: 1 sheet of formal drawings

Application Number (if Known)	International Application Number	Attorney's Docket Number
09/926634	PCT/EP00/04780	MODL3001/JEK

	Calculations	PTO USE ONLY

17. The following fees are submitted:

Basic National Fee *(37 CFR 1.492(a)(1)-(5))*:

☒ Search report has been prepared by the EPO or JPO $890.00
☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* $710.00
☐ No International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)*
but International Search Fee paid to USPTO *(37 CFR 1.445(a)(2))* $740.00
☐ Neither International Preliminary Examination Fee *(37 CFR 1.482)* nor
International Search Fee *(37 CFR 1.445(a)(2))* paid to USPTO $1040.00
☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)*
and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00

ENTER APPROPRIATE BASIC FEE AMOUNT	$ 890.00	

Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(e))*.

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total Claims	18	-20 =		× $18.00		
Independent Claims	4	-3 =	1	× $84.00	$ 84.00	
Multiple Dependent Claims (if applicable)				+ $280.00		
TOTAL OF ABOVE CALCULATIONS					$ 974.00	

Reduction by ½ for filing by small entity, if applicable. Small Entity Status is asserted pursuant to 37 CFR 1.27 for this application.

SUBTOTAL	$ 974.00	

Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(f))*.

TOTAL NATIONAL FEE	$ 974.00	

Fee for recording the enclosed assignment *(37 CFR 1.21(h))*. The assignment must be accompanied by an appropriate cover sheet *(37 CFR 3.28, 3.31)*.   **$40.00** per property.

TOTAL FEES ENCLOSED	$ 974.00	

		Refunded:	
	Amount to be: —	Charged:	

a. ☒ A check in the amount of **$974.00** to cover the fees is enclosed.

b. ☐ Please charge my **Deposit Account Number 02-0200** in the amount of **$_____** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to **Deposit Account Number 02-0200**. A duplicate copy of this sheet is enclosed.

Note: Where an appropriate time limit under *37 CFR 1.494* or *1.495* has not been met, a petition to revive *(37 CFR 1.137(a) or (b))* must be filed and granted to restore the application to pending status.

Customer 23364

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 223124-1176
(703) 683-0500

DATE: 28 November 2001

Respectfully submitted,

J. Ernest Kenney
Attorney for Applicant
Registration Number: 19,179

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

International Patent Application
No. PCT/EP00/04780

PCT/DO/EO/US

International Filing Date: 25 May 2000

Attorney Docket: MODL3001/JEK

Applicant: Albert MÖDL et al.

For: DEVICES AND METHODS FOR BIOMETRIC AUTHENTICATION

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

This paper accompanies documents submitted to establish the U.S. national stage of the above-identified international patent application.

The international patent application was amended under PCT Article 34 and the claims as-amended are annexed to the International Preliminary Examination Report (IPER). A translation of the IPER annex is submitted herewith.

Before calculation of the filing fee and before examination, kindly amend the claims as annexed to the IPER as follows:

IN THE CLAIMS:

Please cancel claims 1 - 15 without prejudice or disclaimer and substitute therefor new claims 16 - 33 as shown on the appended APPENDIX OF CLAIMS.
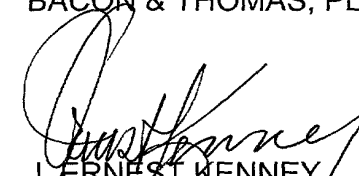
REMARKS

All rights are reserved to the original claimed subject matter. The claims have been amended to reduce the filing fees and to restate the inventive subject matter in clear terms. None of the amendments are intended to narrow any element of the

claims as they stood prior to amendment. Examination of the application as amended is respectfully requested.

Respectfully submitted,
BACON & THOMAS, PLLC

J. ERNEST KENNEY
Attorney for Applicant
Registration No. 19,179

BACON & THOMAS, PLLC

Customer 23364

625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176
Telephone: (703) 683-0500
Facsimile: (703) 683-1080

Date: November 28, 2001

S:\Producer\jek\MODL - MODL3001\preliminary amendment.wpd

International Application No. PCT/EP00/04780
Attorney Docket: MODL3001/JEK

APPENDIX OF CLAIMS

16. A portable data carrier capable of authentication by means of biometric data, comprising a memory in which at least two sets of biometric reference data are stored, and wherein the different sets of reference data are generated from biometric data of a biometric feature using different algorithms.

17. A terminal for authentication by means of biometric data comprising a sensor arranged to detect at least one biometric feature, an I/O device for transferring data, and a control and data processing unit which is arranged to convert biometric data from the sensor which were derived from the at least one detected biometric feature into comparative data by an algorithm, wherein at least two different algorithms are used to convert said biometric data from the sensor into said comparative data.

18. A biometric authentication device comprising:

a portable data carrier capable of authentication by means of biometric data comprising a memory in which at least two sets of biometric reference data are stored, and wherein the different sets of reference data are generated from biometric data of a biometric feature using different algorithms;

a terminal for authentication by means of biometric data comprising a sensor arranged to detect at least one biometric feature, an I/O device for transferring data, and a control and data processing unit which is arranged to convert biometric data from the sensor which were derived from the at least one detected biometric feature into comparative data by an algorithm, wherein at least two different algorithms are used to convert said biometric data from the sensor into comparative data;

wherein said reference data are transferred by the I/O device from the data carrier to the terminal, and

-1-

wherein the control and data processing unit are arranged to check the reference data for a match with the comparative data.

19. The authentication device according to claim 18, wherein the comparative data are transferred by the I/O device from the terminal to the data carrier; and

the data carrier includes a control and data processing unit arranged to check the reference data for a match with the comparative data.

20. The authentication device according to claim 18, wherein the portable data carrier is a smart card.

21. The authentication device according to claim 18, wherein the sets of reference data and the algorithms used for generating the sets of comparative data have a characteristic identification, and wherein reference data and comparative data with the same identification are checked.

22. The authentication device according to claim 18, wherein the at least one detected biometric feature is selected from the group consisting of iris, retina, face, speech, fingerprints and a signature including the writing dynamics determined during signing.

23. A method for authentication by means of biometric data comprising the steps:

deriving and storing several reference data from biometric data of at least one biometric feature using different algorithms;

detecting biometric data;

converting the detected biometric data into comparative data by an algorithm; and

comparing the stored reference data with the converted comparative data for an authentication.

24. The method according to claim 23, wherein the step of converting detected biometric data into comparative data is carried out by using at least two different algorithms.

25. The method according to claim 23, wherein the reference data and/or comparative data or the algorithms generating them have an identification, and only the stored reference data are compared with converted comparative data which have the same identification or only comparative data are converted from the detected biometric data by the algorithm which has the same identification.

26. The method according to claim 23, wherein the at least one biometric feature is selected from the group consisting of iris, retina, face, speech, fingerprints and a signature including the writing dynamics determined during signing.

27. The method according to claim 23, wherein several different sets of reference data are derived and stored, and several different sets of comparative data have been converted from detected biometric data, and wherein the several different sets of reference data are compared with the several different sets of comparative data for authentication.

28. The method according to claim 27, wherein the different sets of reference data and the different sets of comparative data are derived and converted from biometric data of the same kind which have been converted by different algorithms.

29. The method according to claim 27, wherein the conversion of the different sets of reference data and comparative data starts out from different biometric data which have been converted by the same or by different algorithms.

30. The method according to claim 27, wherein upon comparison of several different sets of reference data with several different sets of comparative data, the authentication is decided positively if the majority of comparisons are positive.

31. A terminal according to claim 17, wherein the at least one biometric feature is selected from the group consisting of iris, retina, face, speech, fingerprints and a signature including the writing dynamics determined during signing.

32. A portable data carrier according to claim 16, wherein the portable data carrier is a smart card.

33. A portable data carrier according to claim 16, wherein the biometric feature is selected from the group consisting of iris, retina, face, speech, fingerprints and a signature including the writing dynamics determined during signing.

S:\Producer\jek\MODL - MODL3001\appendix of claims.wpd

Devices and method for biometric authentication

The present invention relates to devices and a method for biometric authentication by means of reference data stored in a memory of a portable data carrier.

Devices and methods for biometric authentication are known and include e.g. the evaluation of unique features such as retina, iris, speech, facial features, fingerprints, signatures with detection of the dynamics during signing, etc. Known methods for biometric authentication have been hitherto limited in their spread above all by the high prices for the sensors used for detecting the biometric features. However, new developments have made sensors available, e.g. fingerprint sensors made of semiconductor materials, which allow cost-effective realizations.

For biometric authentication methods to make their final breakthrough with respect to more widespread use, however, there is a need for standardized generation of reference data or standardization of the reference data for the particular biometric features used for authentication. Different suppliers of methods and devices for biometric authentication have hitherto used algorithms for generating the reference data which normally lead to different reference data which are not interchangeable. This limits the employability of biometric methods to the supplier's particular system.

The problem of the present invention is therefore to provide devices and a method for biometric authentication which are universally employable and not limited to a certain system.

This problem is solved by the features of the independent claims.

The invention starts out from the consideration that the storage of several sets of biometric reference data increases the likelihood of the evaluation of at least one set of stored biometric reference data being possible, so that the desired system-independent authentication is attained. This permits the desired wide spread of biometric authentication.

Another embodiment of the invention involves the advantage that higher security of authentication is guaranteed by checking several of the stored sets of biometric data during authentication.

Further advantages of the invention will result from the following description of an example with reference to figures, and the dependent claims.

Figure 1 shows a system for carrying out the inventive method,

Figure 2 shows a component of the system shown in Figure 1.

The biometric authentication system shown in Figure 1 has portable data carrier 1 introduced into input/output device 2 (I/O device) connected with control and data processing unit 3. Control and data processing unit 3 furthermore has connected thereto sensor 4 for detecting biometric features. Furthermore, control and data processing unit 3 may be provided with a keyboard, display and connection to a background data system, such as a telephone connection or network connection. The latter elements are not shown in Figure 1 because they are not of importance for understanding the present invention. The totality of I/O device 2, data processing unit 3 and sensor 4 is usually referred to as a terminal. I/O device 2, data processing unit 3 and sensor 4 can form one structural unit.

Sensor 4 can detect for example biometric features of the eye, e.g. the iris, as shown. As described above, however, it is also possible to use sensors which detect any other biometric data. Control and data processing unit 3 can be formed for example by microcomputer 3 having in particular memory 3a with at least one non-volatile area. Data carrier 1 used can be formed for example by a smart card having chip 1a with a contact bank. Alternatively, one can use contactless smart card 1 with accordingly designed I/O device 2. Via the contact bank I/O device 2 makes a connection to the circuit components contained in chip 1a of smart card 1 which will be described in more detail below. Instead of a smart card, portable data carrier 1 can also be realized by an optical, magnetic or other suitable storage medium or a combination of storage media. In this case I/O device 2 must be formed accordingly to be able to read the stored data. To simplify the description of the biometric authentication system, however, a smart card will be assumed as portable data carrier 1 in the following by way of example.

To start up the system, smart card 1 is introduced into I/O device 2 and sensor 4 determines biometric features of the user to whom smart card 1 is to be assigned.

The data of the detected biometric features are transferred by I/O device 2 to micro-computer 3 and processed there. A set of reference data is generated from the biometric features or data. The reference data are transferred by microcomputer 3 to I/O device 2, which is also suitable for writing data, and transferred from I/O device 2 to smart card 1.

For processing the biometric data and generating the set of reference data at least one corresponding algorithm, which is known in the art, is stored in memory 3a of microcomputer 3. In order to make several sets of reference data available in smart card 1, several different algorithms for generating reference data can be present in microcomputer 3. It is likewise possible for the user to perform an initialization on different terminals 2, 3, 4, comprising I/O device 2, microcomputer 3 and sensor 4, by which reference data are generated from the biometric features or data detected by sensor 4 by different algorithms. Different terminals 2, 3, 4 can be located for example with different suppliers of applications for smart card 1. Applications refers in this case to areas of use of smart card 1, such as a bank card for making payments, a door opener card for an access system, a key card for an encryption system, etc. For unique identification of the different sets of reference data or the algorithms generating them, each set of reference data can have added thereto a unique identification which designates the algorithm used for generating the set of reference data, for example in the form of a header preceding the set of reference data. The header can contain for example the name of the person who produces the algorithm used or offers it for use.

Figure 2 shows a more detailed view of chip 1a of smart card 1. Chip 1a has interface 10 for I/O device 2 shown in Figure 1, which can be for example of contact-type or contactless design. Such contactless or contact-type smart cards or I/O devices are known. Interface 10 is connected with signal conditioning unit 11 which conditions the data transferred via interface 10 both for transmission and for reception. Signal conditioning unit 11 is connected with controller 12 (which can be formed by a microcomputer) to which memory 13 is connected. At least one area of memory 12 is formed as a nonvolatile memory.

As described above, the determined sets of reference data are transferred by I/O device 2 to smart card 1. They are transferred via interface 10 and signal conditioning unit 11 to microcomputer 12 which stores them in areas provided in the nonvolatile part of memory 13. The different sets of reference data can be identified by means of the above-described headers which are likewise stored in the nonvolatile area of memory 13.

Upon data exchange between smart card 1 and terminal 2, 3, 4 the legitimacy of data exchange of smart card 1 and/or terminal 2, 3, 4 is usually checked. Data exchange itself can be effected in encrypted form. Methods both for encryption and for checking the legitimacy of terminal and/or smart card are known and need not be described in detail here since they are not important in connection with the present invention.

Memory 13 of smart card 1 contains after start-up several different sets of reference data for the evaluated biometric feature, for example reference data of the iris of the smart card user. When the smart card user wants to activate one of the applications of the smart card, he inserts his smart card 1 into I/O device 2 of terminal 2, 3, 4 which may be constructed like terminal 2, 3, 4 shown in Figure 1 and has the features described above in connection with the initialization of smart card 1. The biometric features or data detected by sensor 4 of terminal 2, 3, 4 are converted by at least one algorithm stored in terminal 2, 3, 4 into at least one set of comparative data. Smart card 1 reads the sets of reference data present there in memory 13 by means of I/O device 2 and compares them with at least one set of the comparative data generated from the biometric features or data detected by sensor 2. If a match within the tolerance range of the algorithm used for comparison is ascertained between a set of reference data stored in memory 13 of smart card 1 and at least one set of comparative data generated in terminal 2, 3, 4, smart card 1 is enabled for the particular desired application.

Since the possibly necessary check of all existing sets of reference data in smart card 1 with all sets of comparative data available in terminal 2, 3, 4 is elaborate, use can be made of the above-described headers. Smart card 1 thus transfers a header

together with the set of biometric reference data to indicate the algorithm used for generating the corresponding set of reference data. In terminal 2, 3, 4 the same algorithm is then used for generating the comparative data from the biometric data of the sensor. It is likewise possible that at the request of terminal 2, 3, 4 a set of reference data generated by a certain algorithm is transferred by smart card 1 to terminal 2, 3, 4. The corresponding algorithm is then also used in terminal 2, 3, 4 for generating the comparative data from the biometric data of sensor 4. To facilitate use it may be provided that identifications are added to terminal 2, 3, 4 and to smart card 1 to designate the particular existing sets of reference data and comparative data or algorithms. This makes it immediately apparent to the user whether an identified terminal can at least evaluate one set of reference data existing on his smart card.

Besides the above-described comparison of the reference data with the comparative data in microcomputer 3 of terminal 2, 3, 4, it is also possible to perform the comparison by means of microcomputer 12 of smart card 1.

To increase the security of the employed check of biometric data, it may be provided that several different sets of reference data and comparative data are used for the authentication check. That is, at least two sets of reference data and comparative data generated by different algorithms are evaluated. For this purpose the biometric data detected by sensor 4 in terminal 2, 3, 4 are converted by microcomputer 3 into different sets of comparative data by different algorithms and compared with the sets of reference data from memory 13 of smart card 1. In the process there can be a sequential check of all sets of reference data stored in memory 13 with each set of comparative data, as described above, until a match with the sets of reference data to be checked is determined. By the above-described use of headers the corresponding sets of reference data can also be directly accessed.

In a modification it is possible to decide authentication positively if for example in case of three checked sets of reference data and comparative data a match was ascertained for two sets of reference data and comparative data.

In another modification it is possible that the different sets of reference data and comparative data are generated from the data of different biometric features, e.g.

iris and retina or fingerprint and iris, etc. In this case accordingly suitable sensors must be present. Additionally, different algorithms can also be applied to the different biometric data in this case.

Claims

1. A portable data carrier (1) for authentication by means of biometric data having a memory (13) in which biometric reference data are stored, characterized in that at least two sets of reference data are stored, the different sets of reference data being generated from the biometric data by different algorithms.

2. A terminal (2,3,4) for authentication by means of biometric data having a sensor (4) for detecting biometric features, an I/O device (2) for transferring data, and a control and data processing unit (3) which converts biometric data from the sensor (4) which were derived from the detected biometric features into comparative data by an algorithm, characterized in that at least two different algorithms are used to convert the biometric data from the sensor (4) into comparative data.

3. A portable data carrier (1) and a terminal (2,3,4) according to claims 1 and 2, characterized in that the reference data are transferred by the I/O device (2) from the data carrier (1) to the terminal (2,3,4), and the control and data processing unit (3) checks the reference data for a match with the comparative data.

4. A portable data carrier (1) and a terminal (2,3,4) according to claims 1 and 2, characterized in that the comparative data are transferred by the I/O device (2) from the terminal (2,3,4) to the data carrier (1), the data carrier (1) having a control and data processing unit (12) which checks the reference data for a match with the comparative data.

5. A portable data carrier (1) according to claim 1 or claim 3 or 4, characterized in that the portable data carrier (1) is a smart card.

6. A portable data carrier (1) or a terminal (2,3,4) according to claims 1 or 2 or any of claims 3 to 5, characterized in that the sets of reference data and the algorithms used for generating the sets of comparative data have a characteristic identification, and reference data and comparative data with the same identification are checked.

7. A portable data carrier (1) or a terminal (2,3,4) according to claims 1 or 2 or any of claims 3 to 6, characterized in that the biometric features are iris, retina,

face, speech, fingerprints or a signature and the writing dynamics determined during signing.

8. A method for authentication by means of biometric data wherein

several reference data derived from the biometric data by different algorithms are stored,

biometric data are detected,

the detected biometric data are converted into comparative data by an algorithm, and

the stored reference data are compared with the converted comparative data for authentication.

9. A method according to claim 8, characterized in that the detected biometric data are converted into comparative data by at least two different algorithms.

10. A method according to claim 8 or 9, characterized in that the reference data and/or comparative data or the algorithms generating them have an identification, and only the stored reference data are compared with converted comparative data which have the same identification or only comparative data are converted from the detected biometric data by the algorithm which has the same identification.

11. A method according to any of claims 8 to 10, characterized in that the biometric features are iris, retina, face, speech, fingerprints or a signature and the writing dynamics determined during signing.

12. A method according to any of claims 8 to 11, characterized in that several different sets of reference data are compared with several different sets of comparative data for authentication.

13. A method according to claim 12, characterized in that the conversion of the different sets of reference data and comparative data starts out from biometric data of the same kind which are converted by different algorithms.

14. A method according to claim 12, characterized in that the conversion of the different sets of reference data and comparative data starts out from different biometric data which are converted by the same or by different algorithms.

15. A method according to any of claims 12 to 14, characterized in that upon comparison of several different sets of reference data with several different sets of comparative data the authentication is decided positively if the majority of comparisons is positive.

Fig. 1

1a

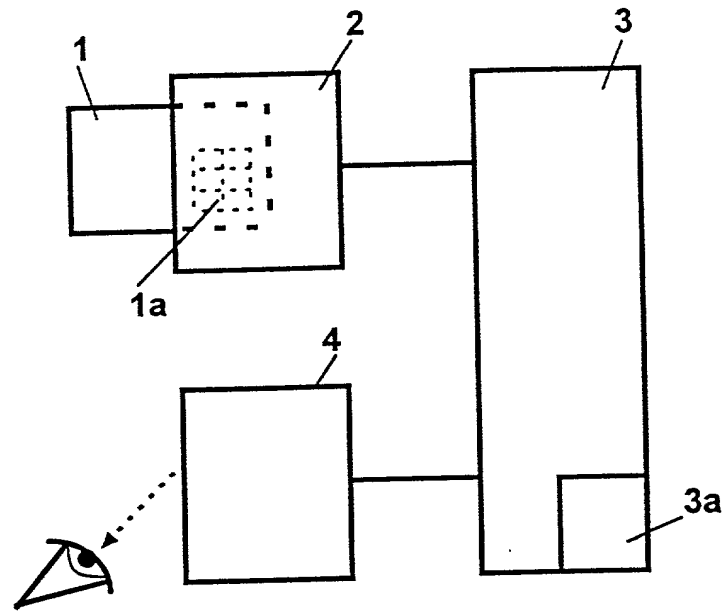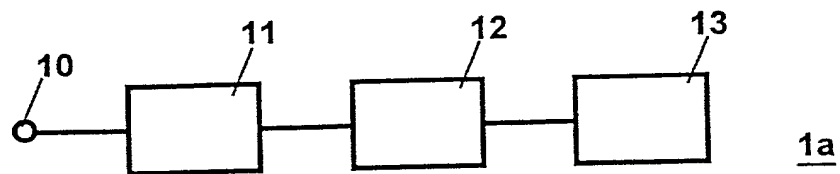**Fig. 2**

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled:

DEVICES AND METHODS FOR BIOMETRIC AUTHENTICATION

the specification of which (check one):

☐ is attached hereto, or ☒ was filed on: **25 May 2000** as U.S. Application Number or PCT International Application Number: **(PCT/EP00/04780) 09/926,634** and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56.* I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	**Country**	**Day/Month/Year Filed**	**Yes**	**No**
199 24 628.9	Germany	28 May 1999	X	

☐ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW.	
Application Number	**Day/Month/Year Filed**

☐ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112,* I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Number	**Filing Date**	**Status - Patented, Pending or Abandoned**

☐ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974; Joseph DeBenedictis, Reg. No. 28,502; Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker Schmitt-Nilson Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to: |||||||||||||||||||||
Customer 23364

BACON & THOMAS, PLLC
625 Slaters Lane - 4ᵗʰ Floor
Alexandria, VA 22314-1176

Telephone Calls to: **J. Ernest Kenney**
(703) 683-0500

FULL NAME OF FIRST OR SOLE INVENTOR **Albert MÖDL**	CITIZENSHIP **Germany**
RESIDENCE ADDRESS Walter-Kollo-Strasse 21, D-86368 Gersthofen, Germany *DEK*	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE *19 Dec. 2001*	SIGNATURE *[signature]*

☒ *See following page(s) for additional joint inventors.*

CONTINUATION OF DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

Page _2_

PRIOR FOREIGN APPLICATION(S) (35 USC §119)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No

PRIOR PROVISIONAL APPLICATIONS 35 U.S. CODE §119(E)	
Application Number	Day/Month/Year Filed

PRIOR U.S. OR PCT INTERNATIONAL APPLICATIONS (35 U.S. CODE §120)		
Application Number	Filing Date	Status - Patented, Pending or Abandoned

FULL NAME OF JOINT INVENTOR **Elmar STEPHAN**	CITIZENSHIP **Germany**
RESIDENCE ADDRESS Danklstrasse 13, D-81371 München, Germany *DEK*	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 21.12.01	SIGNATURE

FULL NAME OF JOINT INVENTOR **Robert MÜLLER**	CITIZENSHIP **Germany**
RESIDENCE ADDRESS Hansjakobstrasse 80, D-81673 München, Germany *DEL*	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 21.12.01	SIGNATURE

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

FULL NAME OF JOINT INVENTOR	CITIZENSHIP
RESIDENCE ADDRESS	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE	SIGNATURE

□ *See following pages for additional joint inventors/priority applications.*